STUDENT NOTE

THE LEGALITY OF WATERING-HOLE-BASED NITS UNDER INTERNATIONAL LAW

John Douglass*

CITE AS: 2 GEO. L. TECH. REV. 67 (2017)

https://perma.cc/KRC5-BZKW

INTRODUCTION: OPERATION PACIFIER

Between February 20 and March 4, 2015, the United States Federal Bureau of Investigation (FBI) administered and monitored a child pornography website in an effort to identify those who accessed the website's illicit content.[1] This website, "Playpen," had more than 150,000

* GLTR Senior Articles Editor; Georgetown Law, J.D. expected 2018; University of California, Los Angeles, B.S. 2007, M.S. 2009.

[1] United States v. Kim, 2017 WL 394498, at *1 n.2 (E.D.N.Y. Jan. 27, 2017); *see also* Gov't's Ex. 1 *In re* the Search of Computers that Access upf45jv3bziuctml.onion, 1:15–SW–89, Search and Seizure Warrant & Application (E.D. Va. Feb. 20, 2015), United States v. Bruce Lorente, No. 2:15–cr–00274–MJP (W.D. Wash. March 7, 2016), ECF No. 48–1 [hereinafter Playpen Warrant].

users worldwide.[2] The FBI's investigation was known as "Operation Pacifier."[3]

Playpen was configured as a Tor hidden service.[4] From a practical perspective, this means that visitors were able to access Playpen without revealing their true identities.[5]

To identify the visitors, the FBI used what is called a "network investigative technique" (NIT).[6] The technique involved configuring the Playpen server to install software on the computers that were used to access it.[7] This style of NIT has been referred to as a "watering hole."[8]

---

[2] *'Playpen' Creator Sentenced to 30 Years*, FED. BUREAU INVESTIGATION (May 5, 2017), https://www.fbi.gov/news/stories/playpen-creator-sentenced-to-30-years [hereinafter FBI Playpen News] [https://perma.cc/XU3L-GMSJ].

[3] *Id.*

[4] *The Playpen Cases: Mass Hacking by U.S. Law Enforcement*, ELEC. FRONTIER FOUND., https://www.eff.org/cases/playpen-cases-mass-hacking-us-law-enforcement [https://perma.cc/93W6-TQN5]; Susan Hennessey & Nicholas Weaver, *A Judicial Framework for Evaluating Network Investigative Techniques*, LAWFARE (July 28, 2016, 10:17 AM), https://www.lawfareblog.com/judicial-framework-evaluating-network-investigative-techniques [https://perma.cc/7FBY-8MGN].

[5] *See Tor: Hidden Service Protocol*, TORPROJECT.ORG, https://www.torproject.org/docs/hidden-services.html.en [https://perma.cc/59TM-FVZ5].

[6] *See* Hennessey & Weaver, *supra* note 4.

[7] *Id.* This paper takes the phrase "install software on a visitor's computer" to include any manner of placing software or code on a visitor's computer. In the United States, district courts have expressed differing views as to whether the NIT's placement of code on a computer is sufficient to trigger Federal Criminal Procedure Rule 41(b)(4)'s procedural requirements regarding the installation of a tracking device. *Compare* United States v. Matish, 193 F. Supp. 3d 585, 613 (E.D. Va. 2016) ("[T]he installation [of the software used to determine the visiting computer's location] did not occur on the government-controlled computer but on each individual computer that entered the Eastern District of Virginia when its user logged into Playpen via the Tor network."), *with* United States v. Kahler, 236 F. Supp. 3d 1009, 1019 (E.D. Mich. 2017) ("[T]he NIT does not actually 'install' a program on the user's computer (in the sense that nothing was left behind on the computer after the NIT finished), it simply requests and receives information."). This paper does not take a view on whether this NIT installed the software in such a manner that would trigger Rule 41 requirements.

[8] *See* NAT'L ASS'N CRIMINAL DEF. LAWYERS, CHALLENGING GOVERNMENT HACKING IN CRIMINAL CASES 6–7 (2017), https://www.nacdl.org/uploadedFiles/files/criminal_defense/national_security/Malware-Guide-3.29.2017.pdf [hereinafter MALWARE GUIDE] (explaining that "[t]he term derives from the concept of poisoning a watering hole where certain animals are known to drink") [https://perma.cc/LB59-24VX].

Once the software was downloaded from Playpen, it transmitted identifying information from those computers to the FBI.[9] This enabled the FBI to identify the site's visitors by locating their computers.[10] The use of this NIT resulted in the software being installed on computers all around the world.[11]

The global reach of watering-hole-based NITs like the one used by the FBI in Operation Pacifier has led some to note the ambiguity of their legality in the context of international law.[12] Indeed, as scholar Ahmed Ghappour explains, the "unilateral[] exercise of law enforcement functions in the territory of another state . . . has not been adequately addressed by courts or scholarship in the context of cyberspace."[13] Professors Orin Kerr and Sean Murphy challenged Ghappour by offering a "plausible" interpretation of contemporary customary international law that law enforcement is permitted to use NITs to determine where a computer is located in order to learn which state to approach for consent in future investigation.[14]

In light of the arguments these parties raise, this paper will address the narrow question of whether watering-hole-based NITs are permissible under international law. In addressing this question, this paper will offer a deeper analysis of the application of customary international law to watering-hole-based NITs than Kerr and Murphy's. This paper will conclude that, while Kerr and Murphy might be right that the use of watering-hole-based NITs is permissible generally, state practice thus far appears to demonstrate their permissibility only in child pornography investigations.

Part I will discuss the technology behind these NITs. Part II will introduce the reader to general concepts of international law that are relevant

---

[9] *See* Hennessey & Weaver, *supra* note 4 (explaining that the identifying details about the computer and the IP address were gathered).

[10] *Id.*

[11] Joseph Cox, *The FBI Hacked Over 8,000 Computers in 120 Countries Based on One Warrant*, MOTHERBOARD (Nov. 22, 2016, 6:18 PM), https://motherboard.vice.com/en_us/article/fbi-hacked-over-8000-computers-in-120-countries-based-on-one-warrant [https://perma.cc/49WH-UF3P]; FBI Playpen News, *supra* note 2 (showing that the investigation has led to 548 international arrests as of May 5, 2017).

[12] Ahmed Ghappour, *Searching Places Unknown: Law Enforcement Jurisdiction on the Dark Web*, 69 STAN. L. REV. 1075, 1108 (2017) ("It is not clear whether (and to what extent) a particular network investigative technique runs afoul of international law").

[13] *Id.* at 1082–83.

[14] *See* Orin S. Kerr & Sean D. Murphy, *Government Hacking to Light the Dark Web: What Risks to International Relations and International Law?*, 70 STAN. L. REV. 58, 68 (2017).

to this discussion. Finally, in Part III, this paper will explain why watering-hole-based NITs are governed by customary international law and are permissible in the context of child pornography investigations.

I. TECHNOLOGY: ANONYMIZATION AND NETWORK INVESTIGATIVE TECHNIQUES

A. Anonymization Using Tor

To understand the need for the NIT used in Operation Pacifier, it is necessary to understand how Internet users can mask their identities using Tor. An Internet user browses the web by using her computer to send and receive discrete bundles of data—called packets—to and from other computers.[15] These packets contain a subset of information—called a header—that is used to route the data from its source to its destination.[16] Within the header is the source Internet Protocol (IP) address of the sender.[17] Under normal circumstances, the source IP address remains unchanged as the packet makes its way to the destination computer and can be read by the destination computer as well as the devices that route the packets to the destination computer.[18] Since all of these routers and the destination computer see the same source IP address, they know where the packet came from and, therefore, can identify the computer that generated the packet.

For both innocent and nefarious reasons, Internet users have sought ways to hide their identities on the web. One tool to do so is the Tor network.[19] The Tor network protects the anonymity of its users by routing packets from a source computer through a series of routers such that each router only sees the IP address of the devices immediately preceding and

---

[15] PRESTON GRALLA, HOW THE INTERNET WORKS 12, 19–20 (8th ed. 2007).

[16] William R. Parkhurst, *Internet Addressing and Routing First Step*, CISCOPRESS (Nov. 5, 2004), http://www.ciscopress.com/articles/article.asp?p=348253&seqNum=4 [https://perma.cc/EB7W-GHZ5].

[17] *Id.*

[18] *See* Farha Ali, *IP Spoofing*, CISCO, http://www.cisco.com/c/en/us/about/press/internet-protocol-journal/back-issues/table-contents-38/104-ip-spoofing.html [https://perma.cc/5AE3-EM2V]; Gralla, *supra* note 15, at 20–21.

[19] *See generally Tor: Overview*, TORPROJECT, https://www.torproject.org/about/overview.html.en [https://perma.cc/7QPQ-AVQ4].

following it in the packet's path.[20] Therefore, while the router that receives the packet from the source computer sees the source computer's IP address, this router will only know the destination IP address of the next router in the packet's path.[21] Similarly, while the last router in the path will know the IP address of the destination computer, it will only know the source IP address of the router preceding it in the packet's path.[22] Since neither the routers in the path nor the destination computer know both the user's source IP address and the destination computer's IP address, there is no way to link the data accessed at the destination computer to the user, and the user is therefore free to obtain this data anonymously.[23]

B. Network Investigative Techniques (NITs)

Because Tor enables user anonymity, law enforcement has used NITs that circumvent Tor and identify users who access illicit material. Broadly speaking, NITs are "methods or tools [the government] uses to access computers of individuals that have taken steps to obscure or mask certain identifying information, like an IP address."[24] Many of these techniques function by "surreptitiously installing software on a target's computer,"[25] which "cause[s] the computer receiving it to transmit data that will help

---

[20] *See* Roger Dingledine, et al., *Tor: The Second-Generation Onion Router*, TORPROJECT, https://svn.torproject.org/svn/projects/design-paper/tor-design.pdf ("Clients choose a path through the network and build a circuit, where each node (or 'onion router' or 'OR') in the path knows its predecessor and successor, but knows no other nodes in the circuit.") [https://perma.cc/CTC6-V8XN].

[21] *See Tor FAQ: How is Tor Different from Other Proxies?*, TORPROJECT, https://www.torproject.org/docs/faq.html.en#Torisdifferent [https://perma.cc/6YPT-MU36].

[22] *See id.*

[23] *See* Playpen Warrant, *supra* note 1, at 11. The foregoing discussion describes how a packet is sent through a normal Tor circuit. Tor also supports a different type of communication path for users that want to advertise their existence to the world while hiding their location. *See generally* TORPROJECT, *supra* note 5 [https://perma.cc/HJP5-R2DY]. Understanding the hidden service protocol is not essential to understanding the issues discussed in this paper.

[24] *What is a "NIT"?*, ELEC. FRONTIER FOUND., https://www.eff.org/pages/playpen-cases-frequently-asked-questions#whatisanit [https://perma.cc/5TWL-WDP2]; United States v. Matish, 193 F. Supp. 3d 585, 594–95 (E.D. Va. 2016) (describing the Playpen NIT as "a set of computer code" used to "obtain identifying information" from computers, the locations of which were otherwise unidentifiable to the FBI).

[25] Devin M. Adams, *The 2016 Amendments to Criminal Rule 41: National Search Warrants to Seize Cyberspace, "Particularly" Speaking*, 51 U. RICH. L. REV. 727, 739 (2017).

identify the computer, its location, other information about the computer, and the user of the computer."[26] This software is known by different names;[27] however, this paper will use the term NIT throughout for consistency.

To understand the application of international law to watering-hole-based NITs like the one used in Operation Pacifier, one must understand the various components of this NIT. These components include: (1) a "generator," (2) an "exploit," (3) a "payload," and (4) a "logging server."[28]

The generator is software that delivers the exploit and the payload to the target computer.[29] The generator also creates a unique identification number, associates it with a logged-in user of the website, and delivers it to the target computer so that the user's activity on a website can be tracked in the website's logs.[30] In the case of a watering-hole attack[31] like that used in Operation Pacifier,[32] the delivery program is run on the server hosting a website and delivers the exploit and the payload to each of the website's visitors.[33]

The exploit is a piece of software that, when run on the target computer, causes the computer to behave in a manner unintended by the user.[34] This unanticipated behavior can include various steps that result in granting a third party—for instance, the government—control over the target computer.[35] While the FBI has managed to keep the precise workings of

[26] Application for Warrant at 1, *In re* Search of Network Investigative Technique ("NIT") for email address texan.slayer@yahoo.com, No. 12–SW–05685–KMT (D. Colo. Dec. 11, 2012).
[27] *See* Brian L. Owsley, *Beware of Government Agents Bearing Trojan Horses*, 48 AKRON L. REV. 315, 316 (2015) (providing the following names for software the Government uses to access a target computer: Trojan device, data extraction software, network investigative technique (NIT), port reader, harvesting program, remote search, Computer and Internet Protocol Address Verifier (CIPAV), and Internet Protocol Address Verifier (IPAV)).
[28] Hennessey & Weaver, *supra* note 4; *see also The Playpen Cases: Frequently Asked Questions*, ELEC. FRONTIER FOUND., https://www.eff.org/pages/playpen-cases-frequently-asked-questions#howdidplaypenmalwarework [https://perma.cc/A33P-LCMS].
[29] *See* ELEC. FRONTIER FOUND., *supra* note 28.
[30] *Id.*
[31] *See generally* MALWARE GUIDE, *supra* note 8, for a discussion of the existing watering-hole attacks as of March 2017.
[32] *See* United States v. Jean, 207 F. Supp. 3d 920, 941 n.22 (W.D. Ark. 2016).
[33] *See* Hennessey & Weaver, *supra* note 4.
[34] ELEC. FRONTIER FOUND., *supra* note 28.
[35] *Id.*

Operation Pacifier's exploit secret,[36] exploits used in similar cases have functioned by taking advantage of vulnerabilities in a user's browser.[37] In one such case, the exploit existed as code on a server.[38] When a user visited a specific website hosted on that server, the user's browser ran the code, which ultimately loaded and executed the NIT's payload on the target computer.[39]

"The payload is the software that conducts the actual search on the visitor's computer."[40] Among the things the payload revealed in Operation Pacifier was the target computer's actual IP address and the unique identifier transmitted to the target computer by the generator.[41]

Finally, the logging server is a computer that collects the data transmitted by the payload.[42] This data can later be analyzed and used as evidence when the government charges the suspect.

As the descriptions above indicate, the generator, exploit, and payload all contain software or data that is run or installed on the target computer in the process of searching that computer. Given the government's assertion that "the identities of the . . . users of [Playpen] would remain unknown without the use of [network] investigative techniques,"[43] the NIT could have searched the computer of a visitor located in any country. Indeed, some of these searches have led to arrests in countries including Israel, Turkey, Peru,

---

[36] *See* Hennessey & Weaver, *supra* note 4. In fact, when faced with the prospect of having to disclose the code to a defendant who was arrested as a result of Operation Pacifier, the government opted to drop the case. Lily Hay Newman, *The Feds Would Rather Drop a Child Porn Case Than Give Up a Tor Exploit*, WIRED (Mar. 3, 2017, 9:00 AM), https://www.wired.com/2017/03/feds-rather-drop-child-porn-case-give-exploit/ [https://perma.cc/P3GX-RW4Y]; Order Dismissing Indictment without Prejudice, United States v. Michaud, No. CR15–5351 (W.D. Wash. Mar. 6, 2017), ECF No. 228.

[37] *See* Dan Goodin, *Firefox 0-Day in the Wild Is Being Used to Attack Tor Users*, ARS TECHNICA (Nov. 29, 2016, 8:50 PM), https://arstechnica.com/information-technology/2016/11/firefox-0day-used-against-tor-users-almost-identical-to-one-fbi-used-in-2013/ [https://perma.cc/LKB2-NM8J].

[38] *See id.*

[39] *See id.*

[40] Hennessey & Weaver, *supra* note 4. The term "search" here includes the process of retrieving data from the user's computer. This paper does not take a stance on whether this process would be considered a "search" in the context of the Fourth Amendment of the United States Constitution.

[41] *See* Playpen Warrant, *supra* note 1, at 33.

[42] Hennessey & Weaver, *supra* note 4.

[43] Playpen Warrant, *supra* note 1, at 22.

Malaysia, Chile, and Ukraine.[44] This means that the government's NIT necessarily installed software on computers in all of these countries.

II. LAW: SOURCES OF INTERNATIONAL LAW

To understand whether cross-border searches like those that occurred during Operation Pacifier are permissible under international law, it is first necessary to determine which provisions of international law govern these searches. Making this determination requires a brief introduction to international law and its sources.

Article 38 of the Statute of the International Court of Justice is generally regarded as listing the sources of international law.[45] It lists the following as primary sources: (1) international conventions, whether general or particular, establishing rules expressly recognized by the relevant states; (2) the general principles of law recognized by civilized nations; and (3) international custom as evidence of a general practice accepted as law.[46] Article 38 also provides that "judicial decisions and the teachings of the most highly qualified publicists of the various nations, [shall provide] subsidiary means for determination of the rules of law."[47]

A. Treaties

Treaties, sometimes called international conventions,[48] consist of state commitments that states make that would not otherwise be legally required of them.[49] These commitments must be executed in good faith,[50] and states are

[44] FBI Playpen News, *supra* note 2.
[45] 1 OPPENHEIM'S INTERNATIONAL LAW § 9, at 24 (Robert Jennings & Arthur Watts eds., 9th ed. 2008) [hereinafter OPPENHEIM].
[46] Statute of the International Court of Justice, art. 38(1)(a)–(c), Oct. 24, 1945, 59 Stat. 1055, 33 U.N.T.S. 933 [hereinafter ICJ Statute].
[47] *Id.* art. 38(1)(d).
[48] The term "treaty" has been used synonymously with the terms "international convention," "international agreement," "general act," and "charter." *See* MALCOLM N. SHAW, INTERNATIONAL LAW 66 (7th ed. 2014).
[49] *See* HUGH THIRLWAY, THE SOURCES OF INTERNATIONAL LAW 7, at 33 (2014).
[50] BIN CHENG, GENERAL PRINCIPLES OF LAW AS APPLIED BY INTERNATIONAL COURTS AND TRIBUNALS 112–14 (1953) (describing the principle of *pacta sunt servanda*); in English, *pacta sunt servanda* approximately translates to "agreements must be kept." *Pacta Sunt Servanda*, BLACK'S LAW DICTIONARY (10th ed. 2014).

generally free to make such commitments so long as they do not require the states to violate certain "peremptory norms."[51]

B. Customary International Law

The second source, customary international law, will be the most applicable to the later discussion of whether watering-hole-based NITs conform with international law. To become customary international law, a rule must be evidenced by consistent state practice and *opinio juris*, where *opinio juris* is: the subjective belief by "the States concerned . . . that they are conforming to what amounts to a legal obligation."[52] The contours of these two required conditions will be explored later in the context of watering-hole-based NITs.

C. Municipal Laws

The final source, general principles of law recognized by civilized nations, consists of municipal laws that are "applicable to [the] relations of states."[53] The application of this source of law in international tribunals has been limited in favor of the application of other sources.[54] In fact, it has been considered by some to be a secondary source of international law.[55] Its purpose is to close gaps in international law, primarily when the tribunal confronts procedural or evidentiary issues.[56] Given the limited applicability of

---

[51] *See, e.g.*, OPPENHEIM, *supra* note 45, § 2 at 7; *see also* Vienna Convention on the Law of Treaties art. 53, *opened for signature* May 23, 1969, 1155 U.N.T.S. 331 (entered into force Jan. 27, 1980) [hereinafter VCLT]. Some examples of "peremptory norms," also known as *jus cogens*, are the prohibition of slavery and the right of a nation to maintain permanent sovereignty over its natural resources. *See* ALEXANDER ORAKHELASHVILI, PEREMPTORY NORMS IN INTERNATIONAL LAW 52, 54 (2008).

[52] *See, e.g.*, OPPENHEIM, *supra* note 45, § 10 at 27–28 (quoting The North Sea Continental Shelf Cases (Ger./Den.; Ger./Neth.), Judgment, 1969 I.C.J. Rep. 3, 44 (Feb. 20)).

[53] *See, e.g.*, *id.* at 36–37.

[54] *See, e.g.*, *id.* at 37–38.

[55] RESTATEMENT (THIRD) OF THE FOREIGN RELATIONS LAW OF THE UNITED STATES § 102(4) (AM. LAW INST. 1987) ("General principles common to the major legal systems, even if not incorporated or reflected in customary law or international agreement, may be invoked as supplementary rules of international law where appropriate.").

[56] SHAW, *supra* note 48, at 70–71.

this source, this paper will only address the legality of watering-hole-based NITs in view of international treaties and customary international law.

III. APPLICATION: PRIMARY SOURCES OF INTERNATIONAL LAW AND WATERING-HOLE-BASED NITS

The first step in determining the permissibility of watering-hole-based NITs is to determine the governing source of international law. This section will first show that no treaties govern the use of these NITs. Then, it will show that the use of such NITs is permissible under the current state of customary international law.

A. Treaties

Currently, there is no treaty that absolutely prohibits cross-border searches like the one used in Operation Pacifier.[57] However, the Council of Europe's Convention on Cybercrime, also known as the Budapest Convention, does contain provisions on how such cross-border searches should be conducted.[58] Specifically, it requires each party to adopt measures that enable it to search computer systems and seize data from within its own territory and provides that other parties may request this data.[59] It also provides that parties may obtain data from persons in another party state "if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data."[60] These provisions instruct state parties on what actions to take when the information they seek is in another party's territory, but they do not expressly address how parties should conduct searches when they do not know the location of a suspect.

The Vienna Convention on the Law of Treaties, which represents a "starting point for any description of the modern law and practice of

---

[57] Ahmed Ghappour, *supra* note 12, at 1118.

[58] *See generally*, Convention on Cybercrime, Nov. 23, 2001, E.T.S. 185. The Convention on Cybercrime has been ratified by fifty-five countries, including the United States. Chart of Signatures and Ratifications of Treaty 185: Convention on Cybercrime, COUNSEL OF EUROPE, http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures [hereinafter Budapest Convention Signatories] [https://perma.cc/W8EA-4D9T].

[59] Convention on Cybercrime, *supra* note 58, arts. 19, 31.

[60] *Id.* art 32.

treaties,"[61] provides that subsequent practice of parties to a treaty shall be taken into account when interpreting the terms of that treaty.[62] In the case of Operation Pacifier, the FBI's watering-hole-based NIT has led to at least 368 arrests in Europe and the dissemination of "[i]ntelligence packages . . . to law enforcement authorities in countries including Colombia, Croatia, Czech Republic, France, Ireland, Italy, Slovakia, Spain, Switzerland and the United Kingdom."[63] All of the listed countries, except Ireland, have signed or ratified the Budapest Convention.[64] Their apparent acquiescence to receiving information from the United States government's search may imply that these parties believe that such a search is not a violation of the treaty.[65] In light of this subsequent state practice, it is ambiguous whether the Budapest Convention proscribes a government's use of watering-hole-based NITs. Therefore, it is necessary to look to customary international law for guidance on the permissibility of such a NIT.

B. Customary International Law

Recall that a rule must manifest itself in (1) state practice and (2) *opinio juris* to become customary international law.[66] In situations involving new technology, it is often impractical to wait for these two conditions to develop with regard to the specific technology. Instead, the legality of actions involving the technology can be analyzed under existing legal frameworks.[67]

---

[61] *See* ANTHONY AUST, MODERN TREATY LAW AND PRACTICE 6 (2000).
[62] VCLT, *supra* note 51, art. 31(3)(b).
[63] *Major Online Child Sexual Abuse Operation Leads to 368 Arrests in Europe*, EUROPOL (May 5, 2017), https://www.europol.europa.eu/newsroom/news/major-online-child-sexual-abuse-operation-leads-to-368-arrests-in-europe [hereinafter Europol Playpen News] [https://perma.cc/7BU8-4U3E].
[64] Budapest Convention Signatories, *supra* note 58.
[65] *Cf.* VCLT, *supra* note 51, art. 31(3)(b) (providing that subsequent practice of parties to a treaty shall be taken into account when interpreting the terms of that treaty).
[66] *See supra* Part II.B.
[67] For a pertinent example, see James E. McGhee, *Cyber Redux: The Schmitt Analysis, Tallinn Manual and US Cyber Policy*, 2 J.L. & CYBER WARFARE 64, 83 (2013), for a description of the International Court of Justice's Nuclear Advisory Opinion, Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J. Rep. 226, 243 (July 8), which ultimately supported the application of existing customary international law regarding the use force to nuclear weapons.

Applying existing legal frameworks to new technology can then result in the creation of new rules or changes to existing rules.[68]

Following the tradition of analyzing actions enabled by new technology under existing customary international law, scholars have considered whether a cross-border computer search would constitute an exercise of a state's enforcement jurisdiction in a foreign territory.[69] This inquiry is significant because customary international law prohibits states from unilaterally exercising enforcement jurisdiction within the boundaries of another state.[70]

Notably, proponents of applying this rule in the computer-search context have left open the possibility that a unilateral cross-border search will not necessarily violate customary international law when law enforcement does not know where the computer is located prior to conducting the search.[71] Others have explicitly stated that the limitations on enforcement jurisdiction in the physical world do not clearly prohibit cross-border computer searches.[72]

Taking the general prohibition on the exercise of a state's enforcement jurisdiction in a foreign territory into consideration, this section of the paper will assess the legality of watering-hole-based NITs under customary international law. It concludes that current state practice and *opinio juris* suggest that such searches are permissible, with the caveat that this acceptance has only been tested in the context of child pornography investigations.

1. State Practice

Current state practice indicates that watering-hole-based NITs in child pornography investigations are likely permissible under customary international law. State practice can be established through action or

---

[68] *See* Colin B. Picker, *A View from 40,000 Feet: International Law and the Invisible Hand of Technology*, 23 CARDOZO L. REV. 149, 156 (2001).

[69] *See, e.g.*, Patricia L. Bellia, *Chasing Bits Across Borders*, 2001 U. CHI. LEGAL F. 35, 61–62 (2001).

[70] *See, e.g.*, RESTATEMENT (THIRD) OF THE FOREIGN RELATIONS LAW OF THE UNITED STATES § 432(2) (AM. LAW INST. 1987); *cf.* S.S. Lotus (Fr. v. Turk.), Judgment, 1927 P.C.I.J. (ser. A) No. 10, at 18 (Sept. 7) ("Now the first and foremost restriction imposed by international law upon a State is that—failing the existence of a permissive rule to the contrary—it may not exercise its power in any form in the territory of another state.").

[71] Bellia, *supra* note 69, at 100.

[72] Jack L. Goldsmith, *The Internet and the Legitimacy of Remote Cross-Border Searches*, 2001 U. CHI. LEGAL F. 103, 115 (2001).

inaction.[73] Inaction is particularly indicative of state practice when a state would be expected to protest the action of another state.[74] Applying this rule to cross-border searches would lead one to expect that when such a search violates international law by infringing upon the sovereignty of another state, the infringed state would protest the search.

As described earlier, Operation Pacifier resulted in cross-border searches in multiple countries and resulted in intelligence packages being created for Colombia, Croatia, Czech Republic, France, Ireland, Italy, Slovakia, Spain, Switzerland, and the United Kingdom.[75] The result of this cross-border search has been 548 international arrests as of May 5, 2017,[76] including arrests in Greece, Denmark, and Chile.[77] Thus, rather than protest the cross-border searches resulting from the watering-hole-based NIT, states have implicitly endorsed such searches by using information obtained from these searches to enforce laws within their own territories.[78] Given the breadth of this search, this lack of protest implies that state practice supports a finding that searches resulting from watering-hole-based NITs are permissible under customary international law.

This was not the first time the U.S. government used a watering-hole-based NIT to conduct a search related to a child pornography investigation.[79] Indeed, the practice was used in 2012 and again in 2013.[80] Moreover, foreign governments helped the United States conduct these investigations.[81] This

---

[73] *See* MICHAEL P. SCHARF, CUSTOMARY INTERNATIONAL LAW IN TIMES OF FUNDAMENTAL CHANGE 35 (2013).

[74] *Id*.

[75] *See* Cox, *supra* note 11; FBI Playpen News, *supra* note 2; Europol Playpen News, *supra* note 63.

[76] FBI Playpen News, *supra* note 2.

[77] Joseph Cox, *Child Porn Sting Goes Global: FBI Hacked Computers in Denmark, Greece, Chile*, MOTHERBOARD (Jan. 22, 2016, 2:01 PM), https://motherboard.vice.com/en_us/article/child-porn-sting-goes-global-fbi-hacked-computers-in-denmark-greece-chile [http://perma.cc/5QRW-DKQX].

[78] *Cf. id.* (noting that Greek and Danish police have made arrests related to Operation Pacifier).

[79] *See* Kim Zetter, *Everything We Know About How the FBI Hacks People*, WIRED (May 15, 2016, 7:00 AM), https://www.wired.com/2016/05/history-fbis-hacking/ [https://perma.cc/XX2T-WXGV].

[80] *Id.*

[81] *See* Kevin Poulsen, *Visit the Wrong Website, and the FBI Could End Up in Your Computer*, WIRED (Aug. 5, 2014, 6:30 AM), https://www.wired.com/2014/08/operation_torpedo/ (describing FBI investigations that were aided by Dutch and French governments)

international help further indicates that states may not object to the use of watering-hole-based NITs to conduct searches, and therefore supports a finding that such searches are permissible under customary international law.

Notably, all of the investigations discussed in this paper were child pornography investigations. That 172 out of 193 members of the U.N. General Assembly are parties to the Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography demonstrates broad international agreement that certain acts related to child pornography are prohibited.[82] Relevant to this paper, the Optional Protocol requires state parties to make illegal the acts of "[p]roducing, distributing, disseminating, importing, exporting, offering, selling or possessing . . . child pornography."[83] Considering the widespread agreement to prohibit these acts, one may reasonably infer that nations might be willing to accept the incursions on their sovereignty caused by watering-hole-based NITs in the limited context of child pornography investigations. Since investigations using watering-hole-based NITs have all been related to child pornography, it is unclear from state practice alone whether watering-hole-based NITs are permissible under international law in other contexts.

2. Opinio Juris

Even though state practice implies that watering-hole-based NITs are permissible under customary international law in the context of child

---

[https://perma.cc/ZU7S-8LLT]; *see also* Kerr & Murphey, *supra* note 14, at 65 (noting that there has been "no sign that the United States government or the American public was offended by the foreign search" after "Australian government hacking broke into computers in the United States" as part of a child pornography investigation).

[82] *Status: Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography*, UNITED NATIONS TREATY COLLECTION, https://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=IV-11-c&chapter=4&lang=en (showing 173 parties to the optional protocol, where one of these parties—the Holy See—is not a member state of the U.N. General Assembly) [https://perma.cc/AUA9-AJ32].

[83] Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography art. 3(1)(c), *adopted* May 25, 2000, T.I.A.S. No. 13,095, 2171 U.N.T.S. 247 [hereinafter Optional Protocol]. Under the Optional Protocol "[c]hild pornography means any representation, by whatever means, of a child engaged in real or simulated explicit sexual activities or any representation of the sexual parts of a child for primarily sexual purposes." *Id.* art. 2(c).

pornography investigations, it is necessary to understand the current state of *opinio juris* to determine what is permissible under customary international law. This is especially true if, as some commentators assert, modern customary international law tends place greater weight on *opinio juris* than state practice.[84]

Recall that for a proposed rule of customary international law to be practiced with the requisite *opinio juris*, "[t]he States concerned must . . . feel that they are conforming to what amounts to a legal obligation."[85] The difficulty with assessing the presence of *opinio juris* is that it requires inferring a state's subjective belief from its actions.[86]

In light of the difficulty of "proving the existence of the *opinio juris*, increasing reference has been made to conduct within the international [organizations]."[87] For example, the International Court of Justice has adopted codifications of international law by the International Law Commission (ILC) as accurate representations of customary international law.[88]

Just as the ILC codifies rules of international law, the NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE) has attempted to codify the rules of international law as they apply to cyber operations. This effort has resulted in the publication of the *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (*Manual*).

It is unclear whether the *Manual* will become an authoritative recitation of customary international law like the ILC codifications. As the *Manual* itself explains, "[the *Manual*] is not an official document, but rather the product . . . of independent experts acting solely in their personal

---

[84] *See* Anthea Elizabeth Roberts, *Traditional and Modern Approaches to Customary International Law: A Reconciliation*, 95 AM. J. INT'L L. 757, 758 (2001). In fact, some scholars have even implied that "instant" customary international law can be formed under certain circumstances given the requisite *opinio juris*. *See* BIN CHENG, STUDIES IN INTERNATIONAL SPACE LAW 136–41 (1997).

[85] OPPENHEIM, *supra* note 45, at 28 (quoting North Sea Continental Shelf, Judgment, 1969 I.C.J. Rep. 3, 44 (Feb. 20)).

[86] *Cf.* H.W.A. THIRLWAY, INTERNATIONAL CUSTOMARY LAW AND CODIFICATION 47–48 (1972) (discussing the difficulty with assigning a precise definition of *opinio juris* and the debate about which evidence is sufficient to prove its existence).

[87] SHAW, *supra* note 48, at 63.

[88] *Id.* (citing Gabčíkovo-Nagymaros Project (Hung/Slovk.), Judgment, 1997 I.C.J. Rep. 7, 38–42, 46 (Sep. 25)).

capacity."[89] Furthermore, "[t]he Manual does not represent the views of the NATO CCD COE, its sponsoring nations, or NATO."[90] However, during the drafting of the *Manual*, over fifty States and international organizations had the opportunity to provide written comments on the proposed *Manual*.[91]

This drafting process is quite like the process by which the ILC drafts its codifications of international law in that the process is meant to identify existing international law,[92] the drafters sit in their individual capacity and not as representatives of their Governments,[93] and the process allows for states to comment on the proposed codification.[94] However, significant differences exist as well. For instance, the members of the ILC are selected by the U.N. General Assembly,[95] whereas the experts who drafted the *Manual* were selected by the NATO CCD COE.[96] This is significant because there is greater state involvement in the selection of the ILC, which may imply that the ILC is more capable of reflecting these state's subjective beliefs than the NATO CCD COE's group of experts. Balancing these considerations, it is unclear whether the *Manual* will be held to accurately represent *opinio juris*.

Even if the *Manual* is taken to reflect *opinio juris* among states, it does not provide clear guidance on the legality of the use of watering-hole-based NITs. In accordance with the customary international law rules regarding enforcement jurisdiction, the *Manual*'s Rule 11 proclaims, "a State may only exercise extraterritorial enforcement jurisdiction in relation to persons, objects, and cyber activities on the basis of (a) a specific allocation of authority under international law, or (b) valid consent by a foreign

---

[89] TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS 2 (Michael N. Schmitt ed., Cambridge University Press 2d ed. 2017) [hereinafter TALLINN MANUAL 2.0].
[90] *Id.*
[91] *Id.* at 6.
[92] *Compare Analytical Guide to the Work of the International Law Commission*, INT'L L. COMM'N, http://legal.un.org/ilc/guide/1_13.shtml [https://perma.cc/N7NQ-DES8], *with* TALLINN MANUAL 2.0, *supra* note 89, at 3.
[93] *Compare Membership: Qualifications and Nationality*, INT'L L. COMM'N, http://legal.un.org/ilc/ilcmembe.shtml#a5 [https://perma.cc/RU9F-Q8AW], *with* TALLINN MANUAL 2.0, *supra* note 89, at 2.
[94] *Compare* G.A. Res. 174 (II), art. 21 (Nov. 17, 1947) [hereinafter ILC Statute], *with* TALLINN MANUAL 2.0, *supra* note 89, at 6.
[95] ILC Statute, *supra* note 94, art. 3.
[96] TALLINN MANUAL 2.0, *supra* note 89, at 1.

Government."[97] The comments that accompany this rule indicate that it is based on the principle that exercising enforcement jurisdiction in another state's territory without the proper authority or consent is a violation of that state's sovereignty, as proscribed by Rule 4.[98] Significantly, the commentary to Rule 4 states that "no consensus could be achieved as to whether . . . a cyber operation that results in neither physical damage nor the loss of functionality amounts to a violation of sovereignty."[99] Given that the watering-hole-based NIT used in Operation Pacifier only reported data back to the government and does not seem to have caused physical damage or loss of functionality, it seems as though this style of NIT fits precisely in the gray area of the Rule 4 commentary.

Nevertheless, the Rule 4 commentary is significant because it demonstrates that NATO CCD COE's group of experts did not overlook the issue as to whether a cyber operation that results in neither physical damage nor the loss of functionality could amount to a violation of sovereignty. Rather, the experts considered the issue and failed to reach consensus. This leaves ambiguous the state of *opinio juris* regarding watering-hole-based NITs that neither cause physical damage nor loss of functionality.

3. The Rule: Combining State Practice and *Opinio Juris*

Given the ambiguous state of *opinio juris* regarding the use of watering-hole-based NITs, state practice offers the only guidance as to the current state of customary international law. As explained above, the fact that countries have not objected to the FBI's use of the watering-hole-based NIT and have themselves used information from it to prosecute offenders implies that the use of these types of NITs is permissible under customary international law—at least in the context of child pornography investigations.

Indeed, the apparent acquiescence to these searches functions as a form of consent, which, as mentioned above, is one way in which a state can be permitted to exercise extraterritorial enforcement jurisdiction. Because this implied consent, which is demonstrated by state practice, is limited to a specific type of NIT being used to investigate a specific type of act, sovereigns can be confident that extraterritorial searches in their territories

[97] *Id.* at 66 (quoting Rule 11).
[98] *Id.* at 66–67.
[99] *Id.* at 21 (quoting Rule 4 cmt. 14).

will be limited in scope and impact. Therefore, the use of watering-hole-based NITs to conduct child pornography investigations—and perhaps investigations of other acts that are widely prohibited by the international community—seems to strike the proper balance between law enforcement needs and the right of a state to preclude other states from exercising enforcement jurisdiction within its territory.

CONCLUSION

Watering-hole-based NITs like the one used in Operation Pacifier provide a valuable tool in preventing cybercrime as they enable law enforcement to locate criminals who have anonymized their presence on the Internet. Since it is possible for cybercriminals to hide their locations using anonymization tools, continued use of these watering-hole-based NITs will invariably continue to result in cross-border computer searches. Given the current state practice of using watering-hole-based NITs in the context of child pornography investigations and the apparent acquiescence to the cross-border searches that result from these NITs, such searches are likely permissible under international law.